PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-194657
(43)Date of publication of application : 14.07.2000

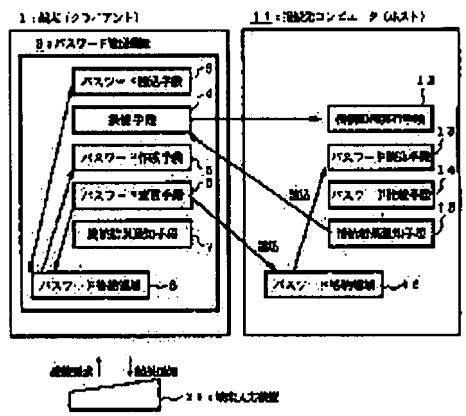
(51)Int.Cl. G06F 15/00

(21)Application number : 10-373606
(22)Date of filing : 28.12.1998

(71)Applicant : FUJITSU LTD
(72)Inventor : SATAKE SHUICHI

(54) CONNECTING DEVICE AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To shorten the life duration of a connection password and to disable connection with a computer from other devices by sending a newly generated password for connection to an opposite computer and changing the password, and updating a stored password for connection.
SOLUTION: When an identification code and a password, which have been inputted, are matched with held values, respectively, a password managing device 2 is made to start a processing and a connecting means 4 transmits a password for connection and an identification code read out of a password storage area 8 to a connection destination to make a connection, and then data are transmitted and received. Further, a password generating means 5 generates a new password for connection with a random number according to the password for connection, sends the password for connection to the connection destination to change the password, and updates the password for connection in the password storage area 8. A new password is generated with a random number according to ≥1 of the password for connection, connection time, and connection frequency.



LEGAL STATUS

[Date of request for examination] 09.03.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開2000－194657

（P2000－194657A）

(43)公開日　平成12年７月14日(2000.7.14)

(51)Int.Cl.^{7}	識別記号	ＦＩ	テーマコード*(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00　３３０Ｂ	５Ｂ０８５

審査請求　未請求　請求項の数４　ＯＬ　（全 ６ 頁）

(21)出願番号　特願平10－373606

(22)出願日　平成10年12月28日(1998.12.28)

(71)出願人　000005223

富士通株式会社

神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　佐竹　修一

富山県婦負郡八尾町保内二丁目２番１　株式会社富山富士通内

(74)代理人　100089141

弁理士　岡田　守弘

Ｆターム(参考)　5B085 AE03

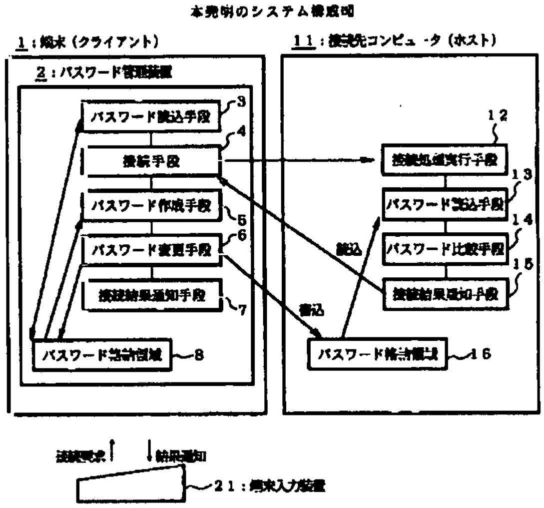
(54)【発明の名称】　接続装置および記録媒体

(57)【要約】　（修正有）

【課題】　識別コードとパスワードで他のコンピュータに接続し、接続毎に接続パスワードを自動変更することで、他の装置からコンピュータに接続不可とする。

【解決手段】　入力された識別コードおよびパスワードが保持している値とそれぞれ一致したときに処理開始させる手段と、接続用パスワードを記憶する記憶手段と、手段によって処理開始され、記憶手段から読み出した接続用パスワードと識別コードを相手のコンピュータに送信して接続する手段と、接続用パスワードをもとに乱数によって新たな接続用パスワードを生成する手段と、生成された新たな接続用パスワードを相手のコンピュータに送信してパスワードを変更させると共に記憶手段が記憶する接続用パスワードを更新する手段とを備えるように構成する。

本発明のシステム構成図



【特許請求の範囲】

【請求項１】識別コードおよびパスワードを用いて他のコンピュータに接続する接続装置において、
入力された識別コードおよびパスワードが保持している値とそれぞれ一致したときに処理開始させる手段と、
接続用パスワードを記憶する記憶手段と、
上記手段によって処理開始され、上記記憶手段から読み出した接続用パスワードと識別コードを相手のコンピュータに送信して接続する手段と、
上記接続用パスワードをもとに乱数によって新たな接続用パスワードを生成する手段と、
上記生成された新たな接続用パスワードを相手のコンピュータに送信してパスワードを変更させると共に上記記憶手段が記憶する接続用パスワードを更新する手段とを備えたことを特徴とする接続装置。

【請求項２】上記接続用パスワードと接続時間、接続回数の１つ以上とをもとに乱数によって新たなパスワードを生成することを特徴とする請求項１記載の接続装置。

【請求項３】上記相手のコンピュータと接続毎に上記接続用パスワードを更新することを特徴とする請求項１あるいは請求項２記載の接続装置。

【請求項４】入力された識別コードおよびパスワードが保持している値とそれぞれ一致したときに処理開始させる手段と、
接続用パスワードを記憶する記憶手段と、
上記手段によって処理開始され、上記記憶手段から読み出した接続用パスワードと識別コードを相手のコンピュータに送信して接続する手段と、
上記接続用パスワードをもとに乱数によって新たな接続用パスワードを生成する手段と、
上記生成された新たな接続用パスワードを相手のコンピュータに送信してパスワードを変更すると共に上記記憶手段が記憶する接続用パスワードを更新する手段として機能させるプログラムを記録したコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、識別コードおよびパスワードを用いて他のコンピュータに接続する接続装置および記録媒体に関するものである。

【０００２】

【従来の技術】従来、コンピュータとコンピュータとを接続する際の資格確認として、オペレータを判断するための識別コードとパスワードを接続要求元の端末から入力し、接続先のコンピュータ側で事前に登録されている識別コードとパスワードとを一致するかの比較処理を行い、一致する場合に接続を許可していた。

【０００３】そして、パスワードは接続要求元の端末からオペレータが随時変更することで、第三者による盗用が発生しないようにしていた。

【０００４】

【発明が解決しようとする課題】しかし、従来の上述した識別コードとパスワードを用いた資格確認手法では、オペレータがパスワードを記憶する関係で覚えやすい、誕生日や電話番号などを用いることが多く、オペレータに関係したものとなりがちで、頻繁に同一のパスワードを使用すると、何度かのパスワードの入力によって第三者に検出取得され易いという問題があった。

【０００５】本発明は、これらの問題を解決するため、コンピュータにパスワード管理装置を設けてオペレータは識別コードとパスワードでパスワード管理装置を起動し、パスワード管理装置は接続パスワードを持ってこれで他のコンピュータには接続し、接続毎に乱数により接続パスワードを自動変更することで、接続パスワードの寿命を短くかつ他の装置からコンピュータに接続不可とすることを目的としている。

【０００６】

【課題を解決するための手段】図１を参照して課題を解決するための手段を説明する。図１において、パスワード管理装置２は、パスワードおよび識別コードで処理開始し、内部に保持する接続用パスワードと識別コードで接続先のコンピュータと接続したり、接続毎に新たな接続用パスワードを生成して更新したりなどするものであって、接続手段４、パスワード作成手段５、パスワード格納領域８などから構成されるものである。

【０００７】接続手段４は、接続用パスワードおよび識別コードを接続先に送信して接続するものである。パスワード作成手段５は、接続用パスワードと接続時間、接続回数などをもとに乱数によって新たな接続用パスワードを生成するものである。

【０００８】パスワード格納領域８は、接続用パスワードなどを格納する領域である。次に、動作を説明する。パスワード管理装置２が入力された識別コードおよびパスワードと保持している値とそれぞれ一致したときに処理開始され、当該パスワード管理装置２を構成する接続手段４がパスワード格納領域８から読み出した接続用パスワードと識別コードを接続先に送信して接続してデータの送受信を行うと共に、パスワード作成手段５が接続用パスワードをもとに乱数によって新たな接続用パスワードを生成し、生成した新たな接続用パスワードを接続先に送信してパスワードを変更させると共にパスワード格納領域８の接続用パスワードを更新するようにしている。

【０００９】この際、接続用パスワードと接続時間、接続回数の１つ以上とをもとに乱数によって新たなパスワードを生成するようにしている。また、接続先と接続毎に接続用パスワードを更新するようにしている。

【００１０】従って、コンピュータにパスワード管理装置２を設けてオペレータは識別コードとパスワードでパスワード管理装置２を処理開始し、パスワード管理装置

2は接続パスワードを持ってこれで他のコンピュータには接続し、接続毎に乱数により接続パスワードを自動変更することにより、接続パスワードの寿命を短くかつ他の装置から接続先のコンピュータに接続不可とすることが可能となる。

【0011】

【実施例】次に、図1から図5を用いて本発明の実施の形態および動作を順次詳細に説明する。

【0012】図1は、本発明のシステム構成図を示す。図1において、端末1は、クライアント側のコンピュータであって、端末入力装置21を利用者が操作して接続先コンピュータ11に接続しデータ通信を行い各種処理を行うものであって、ここでは、パスワード管理装置2を介して接続先コンピュータ11と接続してデータ通信を行って各種処理を行うものである。

【0013】パスワード管理装置2は、利用者が端末入力装置21を操作して識別コードとパスワードを入力して予め登録した値とそれぞれ一致して資格OKとなると、起動して接続先コンピュータ11に識別コードと接続毎に異なる接続用パスワードを送信して接続したりなどのセキュリティを管理するものであって、パスワード読込手段3、接続手段4、パスワード作成手段5、パスワード変更手段6、接続結果通知手段7、およびパスワード格納領域8などから構成されるものである。

【0014】パスワード読込手段3は、パスワード格納領域8から接続用パスワードなどを読み込むものである。接続手段4は、識別コードと接続用パスワードをもとに接続先コンピュータ11と接続するものである（図3を用いて後述する）。

【0015】パスワード作成手段5は、接続用パスワードを自動作成するものである（図3から図5を用いて後述する）。パスワード変更手段6は、パスワード格納領域8に格納されている旧の接続用パスワードを、自動作成した接続用パスワードで更新したりなどするものである。

【0016】接続結果通知手段7は、接続先コンピュータ11と接続した結果を、端末入力装置21に通知したりなどするものである。パスワード格納領域8は、接続用パスワードを格納して保持するものである。

【0017】接続先コンピュータ11は、端末1から接続して各種サービスの提供を行うものであって、ここでは、接続処理実行手段12、パスワード読込手段13、パスワード比較手段14、接続結果通知手段15、およびパスワード格納領域16などから構成されるものである。

【0018】接続処理実行手段12は、端末1からの接続要求に対する処理を行うものである。パスワード読込手段13は、パスワード格納領域16から識別コードに対応する接続用パスワードを読み込むものである。

【0019】パスワード比較手段14は、端末1から受信した接続用パスワードと、パスワード格納領域16から読み込んだ当該識別コードの接続用パスワードとを比較し、一致するかいなかをチェックするものである。

【0020】接続結果通知手段15は、パスワード比較手段14によって比較した結果（OK，あるいはNG）などを通知するものである。パスワード格納領域16は、識別コードに対応づけて接続用パスワードを格納して保存するものである。

【0021】端末入力装置21は、利用者が自己の識別コードとパスワードとを入力して端末1に接続してパスワード管理装置2を起動し、当該パスワード管理装置2に依頼して接続先コンピュータ11に接続し、当該接続先コンピュータ11から各種サービスの提供を受けるものである。

【0022】次に、図2のフローチャートの順番で図1の構成の動作を詳細に説明する。図2は、本発明の動作説明フローチャートを示す。図2において、S1は、識別コードを入力する。

【0023】S2は、起動用パスワードを入力する。これらS1、S2は、例えば後述する図3の画面上で利用者が識別コードの欄とパスワードの欄にそれぞれ図示のように入力し、図示外の実行キーを押下する。

【0024】S3は、パスワード確認する。これは、S1、S2で入力された識別コードとパスワードと、これを受信した図1の端末1が予め登録されている識別コードに対応するパスワードとを比較し、一致するか確認する。一致した場合には、S4に進む。不一致の場合には、予め登録された識別コードとパスワードとが一致しないので、エラーを表示し、再入力を促すなどする。

【0025】S4は、接続用パスワードを読み込む。これは、S3の一致で、利用者からの識別コードとパスワードのチェックがOKとなったので、図1のパスワード管理装置2が起動され、当該パスワード管理装置2を構成するパスワード読込手段3がパスワード格納領域8から接続用パスワードを読み込む。

【0026】S5は、パスワードと識別コードを送信する。これは、S5で読み込んだ接続用パスワードと識別コードを、接続先コンピュータ11に向けて送信する。S6は、パスワード確認する。これは、S5で送信された接続用パスワードと識別コードを受信した接続先コンピュータ11のパスワード比較手段14がパスワード格納領域16から読み込まれた当該識別コードの接続用パスワードとを比較し、一致するかいなかを判別する。一致した場合には、S7に進む。不一致の場合には、エラーとして接続処理を中止などする。

【0027】S7は、S6の一致と判明してパスワードのチェックOKとなったので、コンピュータ接続する。これは、接続先コンピュータ11が端末1と接続する。S8は、旧パスワードと接続時間から乱数を作成する。これは、図1のパスワード管理装置2を構成するパスワ

ード作成手段５が旧の接続用パスワードと接続時間から乱数を作成する。

【００２８】Ｓ９は、接続用パスワードを作成する。これは、Ｓ８で作成した乱数をもとに接続用パスワードを作成する。Ｓ１０は、接続パスワードを変更する。これは、図１のパスワード変更手段６が新たに作成した接続用パスワードを接続先コンピュータ１１に送信してパスワード格納領域１６の旧の接続用パスワードを更新（変更）させると共に、パスワード格納領域８の旧の接続用パスワードを更新（変更）する。

【００２９】以上によって、端末１を構成するパスワード管理装置２が接続先コンピュータ１１に接続するときに、接続用パスワードを用いて利用者の確認（識別コードとパスワードによる本人確認）を行って接続しサービスの提供を受けと共に、接続用パスワードを新たに作成して端末１側のパスワード管理装置２内の接続用パスワードおよび接続先コンピュータ１１内の接続用パスワードを同期して更新（変更）することにより、接続毎に接続用パスワードが自動的に利用者が意識することなく変更され、第三者による接続用パスワードを秘密裏に取得しても次回には異なる接続用パスワードとなり長期に渡る盗用を完全に防止することが可能となると共に盗用して接続すると接続用パスワードが変更されてしまい、真正の利用者（パスワード管理装置２）から接続用パスワードを使って接続しようとしても不可となり、盗用されたことを知ることが可能となる。

【００３０】図４は、本発明の接続用パスワード変更処理フローチャートを示す。図４において、Ｓ２１は、パスワードの変更開始する。これは、図１のパスワード管理装置２が接続用パスワードの変更処理の開始を行う。

【００３１】Ｓ２２は、旧のパスワードの入力を行う。Ｓ２３は、新のパスワードの入力を行う。Ｓ２４は、新のパスワードの格納を行う。この際、Ｓ２２で入力された旧のパスワードが図１のパスワード格納領域８に格納されている現パスワードと一致したときにＯＫとし、新のパスワード（接続用パスワード）をパスワード格納領域８に格納し、接続用パスワードを変更（更新）する。尚、図１の接続先コンピュータ１１内のパスワード格納領域１６に格納されている接続用パスワードを変更（更新）する場合も同様に、旧の接続用パスワードが一致したときに新の接続用パスワードで変更（更新）する。

【００３２】以上によって、旧の接続用パスワードが一致したときに接続毎に作成した新の接続用パスワードでパスワード格納領域８，１６の接続用パスワードを変更（更新）することにより、第三者によって接続用パスワードが更新されないようにすることが可能となる。

【００３３】図５は、本発明の接続用パスワードの作成説明図を示す。図５において、旧パスワードは、現在使用する接続用パスワードである。接続依頼時間は、例えば図１のパスワード管理装置２が接続先コンピュータ１１に接続依頼した時間であって、YYMMDDHHMMSS（年月日時分秒ミリ秒）であって、常に変化する値の例である。

【００３４】接続回数は、例えば図１のパスワード管理装置２が接続先コンピュータ１１に接続した回数であって、接続毎に変化する値の例である。乱数発生装置３１は、旧パスワード（旧の接続用パスワード）、接続依頼時間、接続回数をもとに乱数を発生する公知の乱数発生装置である。

【００３５】新パスワードは、乱数発生装置３１によって、旧パスワード、接続依頼時間、および接続回数をもとに発生された乱数から生成された新たな接続用パスワードである。

【００３６】以上のように、旧パスワード（旧の接続用パスワード）、常に変化する接続依頼時間、更に、接続毎に変化する接続回数をもとに乱数を発生して新パスワード（新たな接続用パスワード）を自動作成することが可能となる。

【００３７】

【発明の効果】以上説明したように、本発明によれば、コンピュータにパスワード管理装置２を設けてオペレータは識別コードとパスワードでパスワード管理装置２を処理開始させ、パスワード管理装置２は接続パスワードを持ってこれで他のコンピュータには接続し、接続毎に乱数により接続パスワードを自動変更する構成を採用しているため、接続パスワードの寿命を短くし、かつ他の装置から接続先のコンピュータに接続不可とすることができ、接続時の機密を効果的に高めることが可能となる。これらにより、

（１）　接続毎に接続用パスワードが自動変更されるため、接続時の機密性を高めることが可能となると共に、盗用されても盗用できるのは利用者が次に接続するまでのみと短時間に制限できる。

【００３８】（２）　利用者のパスワードが盗用されても、当該利用者が使用する端末１のパスワード管理装置２が接続毎に自動変更する接続用パスワードを保持するため、当該利用者のパスワードを取得して使用しようとしても他の端末では使えなく、接続時の機密性を高めることが可能となる。

【００３９】（３）　端末１にパスワード管理装置２を付加するのみで、本発明を実現でき、利用者の持つ従来型のパスワードに加えて、接続毎に自動的に変更される第２の接続用パスワードで接続先コンピュータ１１に接続でき、当該接続用パスワードは利用者が知る必要がなく、覚えがたい乱数を使うことができ、予測が困難となり、接続時の機密性を大幅に高めることが可能となる。

【図面の簡単な説明】

【図１】本発明のシステム構成図である。

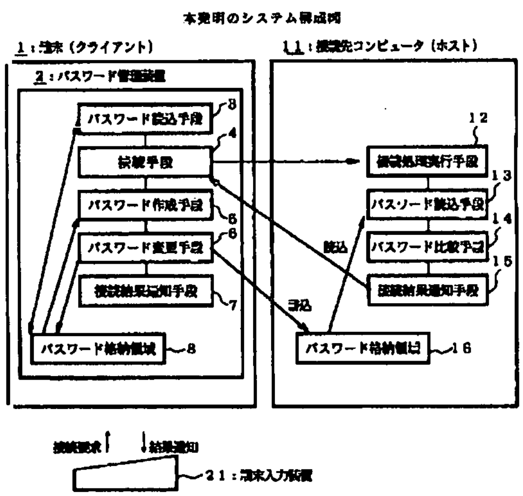
【図２】本発明を動作説明フローチャートである。

【図３】本発明を画面例である。

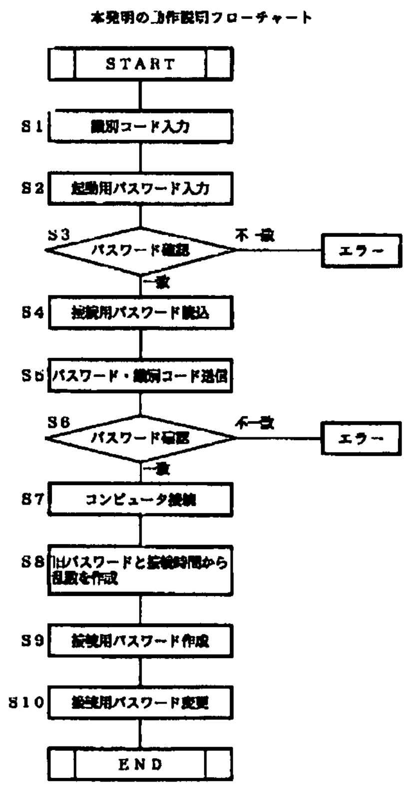
【図４】本発明を接続用パスワード変更処理フローチャ

ートである。
【図5】本発明の接続用パスワードの作成説明図である。
【符号の説明】
1：端末（クライアント）
2：パスワード管理装置
3：パスワード読込手段
4：接続手段
5：パスワード作成手段
6：パスワード変更手段
7：接続結果通知手段
8：パスワード格納領域
11：接続先コンピュータ
12：接続処理実行手段
13：パスワード読込手段
14：パスワード比較手段
15：接続結果通知手段
16：パスワード格納領域
21：端末入力装置
31：乱数発生装置

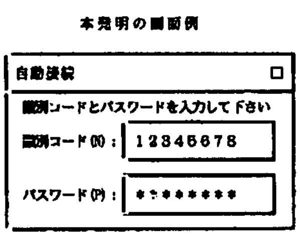
【図1】



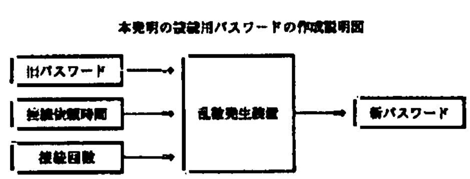
【図2】



【図3】

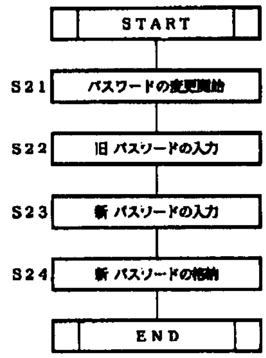


【図5】



【図4】

本発明の接続用パスワード変更処理フローチャート



CLAIMS

[Claim(s)]
[Claim 1] In the contact connected to other computers using identification code and a password The means which carries out processing initiation when in agreement with the value which the identification code and the password which were entered hold, respectively, A storage means to memorize the password for connection, and a means to transmit the password for connection and identification code which processing initiation was carried out and were read from the above-mentioned storage means with the above-mentioned means to a partner's computer, and to connect, A means to generate the new password for connection with a random number based on the above-mentioned password for connection, The contact characterized by having a means to update the password for connection which the above-mentioned storage means memorizes while transmitting the new password for connection by which generation was carried out [above-mentioned] to a partner's computer and making a password change.
[Claim 2] The contact according to claim 1 characterized by generating a new password with a random number based on one or more of the above-mentioned password for connection, a connect time, and the counts of connection.
[Claim 3] Claim 1 characterized by updating the above-mentioned password for connection for every connection with the above-mentioned partner's computer, or a contact according to claim 2.
[Claim 4] The means which carries out processing initiation when in agreement with the value which the identification code and the password which were entered hold, respectively, A storage means to memorize the password for connection, and a means to transmit the password for connection and identification code which processing initiation was carried out and were read from the above-mentioned storage means with the above-mentioned means to a partner's computer, and to connect, A means to generate the new password for connection with a random number based on the above-mentioned password for connection, The record medium which recorded the program operated as a means to update the password for connection which the above-mentioned storage means memorizes while transmitting the new password for connection by which generation was carried out [above-mentioned] to a partner's computer and changing a password and in which computer reading is possible.

[Translation done.]

* NOTICES *

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the contact and record medium which are connected to other computers using identification code and a password.
[0002]
[Description of the Prior Art] The identification code and the password for judging an operator were entered from the terminal of connection-request origin as a rating check at the time of connecting a computer and a computer conventionally, comparison processing in agreement in the identification code registered in advance by the computer side of a connection place and a password was performed, and connection was permitted when in agreement.
[0003] And he was trying for the surreptitious use by the third party not to generate a password because an operator changes at any time from the terminal of connection-request origin.
[0004]
[Problem(s) to be Solved by the Invention] However, by the rating check technique using the conventional identification code and the conventional password which were mentioned above, when the operator tended to become a thing related to an operator and used the same password frequently, using a birthday, the telephone number, etc. which are easy to memorize by the relation which memorizes a password in many cases, the third party had the problem that detection acquisition was easy to be carried out, by the input of that password how many times.
[0005] In order that this invention may solve these problems, password management equipment forms in a computer, an operator starts password management equipment with identification code and a password, and password management equipment connects to other computers now with a connection password, and it is making an automatic change of the connection password with a random number for every connection, and it aims at making the life of a connection password impossible [connection with a computer] from other short equipments.
[0006]
[Means for Solving the Problem] With reference to drawing 1 , The means for solving a technical problem is explained. connecting password management equipment 2 with the computer of a connection place in drawing 1 by the password for connection and identification code which carry out processing initiation by the password and identification code and which are held inside, or generating the new password for connection for every connection, and updating **** -- etc. -- it carries out and consists of a connecting means 4, a password creation means 5, a password storing field 8, etc.
[0007] A connecting means 4 transmits the password for connection, and identification code to a connection place, and is connected. The password creation means 5 generates the new password for connection with a random number based on the password for connection, a connect time, the count of connection, etc.
[0008] The password storing field 8 is a field which stores the password for connection etc. Next, actuation is explained. Processing initiation is carried out when in agreement with the identification code

and the password into which password management equipment 2 was inputted, and the value currently held, respectively. While the connecting means 4 which constitutes the password management equipment 2 concerned transmits the password for connection and identification code which were read from the password storing field 8 to a connection place, connects and transmits and receives data While the password creation means 5 transmits the new password for connection which generated the new password for connection and was generated to a connection place and makes a password change with a random number based on the password for connection, he is trying to update the password for connection of the password storing field 8.

[0009] Under the present circumstances, he is trying for a random number to generate a new password based on one or more of the password for connection, a connect time, and the counts of connection. Moreover, he is trying to update the password for connection for every connection with a connection place.

[0010] Therefore, it becomes that it is possible to make the life of a connection password impossible [connection with the computer of a connection place] from other short equipments by forming password management equipment 2 in a computer, and an operator doing processing initiation of the password management equipment 2 with identification code and a password, and connecting password management equipment 2 to other computers now with a connection password, and making an automatic change of the connection password with a random number for every connection.

[0011]

[Example] Next, the gestalt of operation of this invention and actuation are explained to a detail one by one using drawing 5 from drawing 1 .

[0012] Drawing 1 shows system configuration drawing of this invention. In drawing 1 , it is the computer of a client side, and a user operates the terminal input device 21, it connects with the connection place computer 11, and a terminal 1 performs data communication, performs various processings, it connects with the connection place computer 11 through password management equipment 2, and it performs data communication, and performs various processings here.

[0013] If password management equipment 2 serves as Rating O.K. respectively in accordance with the value which the user operated the terminal input unit 21, entered identification code and a password, and registered beforehand It is what manages security. transmitting a password for connection which starts and is different from identification code for every connection to the connection place computer 11, and connecting **** -- etc. -- It consists of the password reading means 3, a connecting means 4, the password creation means 5, a password change means 6, an advice means 7 of a connection result, a password storing field 8, etc.

[0014] The password reading means 3 reads the password for connection etc. from the password storing field 8. A connecting means 4 is connected with the connection place computer 11 based on identification code and the password for connection (it mentions later using drawing 3).

[0015] The password creation means 5 carries out automatic creation of the password for connection (it mentions later using drawing 5 from drawing 3). that the password change means 6 updates the old password for connection stored in the password storing field 8 with the password for connection which carried out automatic creation **** -- etc. -- it carries out.

[0016] that the advice means 7 of a connection result notifies the result linked to the connection place computer 11 to the terminal input unit 21 **** -- etc. -- it carries out. The password storing field 8 stores and holds the password for connection.

[0017] It connects from a terminal 1, and the connection place computer 11 offers various services, and consists of the connection processing activation means 12, the password reading means 13, a password comparison means 14, an advice means 15 of a connection result, a password storing field 16, etc. here.

[0018] The connection processing activation means 12 performs processing to the connection request from a terminal 1. The password reading means 13 reads the password for connection corresponding to identification code from the password storing field 16.

[0019] The password comparison means 14 compares the password for connection received from the terminal 1 with the password for connection of the identification code concerned read from the password

storing field 16, and checks the inside of a paddle in agreement.
[0020] The advice means 15 of a connection result notifies the result (O.K. or NG) compared with the password comparison means 14. The password storing field 16 is matched with identification code, and stores and saves the password for connection.
[0021] Password management equipment 2 is started, and the password management equipment 2 concerned is requested, it connects [a user enters self identification code and password and it connects with a terminal 1, and] with the connection place computer 11, and the terminal input unit 21 receives offer of various services from the connection place computer 11 concerned.
[0022] Next, the sequence of the flow chart of drawing 2 explains actuation of the configuration of drawing 1 to a detail. Drawing 2 shows the explanation flow chart of this invention of operation. In drawing 2 , S1 inputs identification code.
[0023] S2 enters the password for starting. A user inputs these [S1 and S2] into the column of identification code, and the column of a password like a graphic display on the screen of drawing 3 mentioned later, for example, respectively, and they carry out the depression of the Enter key besides a graphic display.
[0024] S3 carries out a password check. This compares the identification code and the password which were entered by S1 and S2 with the password corresponding to the identification code into which the terminal 1 of drawing 1 which received this is registered beforehand, and checks whether it is in agreement. When in agreement, it progresses to S4. Since the identification code and the password which were registered beforehand are not in agreement in the case of an inequality, an error is displayed and it carries out urging reinput etc.
[0025] S4 reads the password for connection. This is coincidence of S3, since the check of the identification code from a user and a password was set to O.K., the password management equipment 2 of drawing 1 is started, and a password reading means 3 to constitute the password management equipment 2 concerned reads the password for connection from the password storing field 8.
[0026] S5 transmits a password and identification code. This turns to the connection place computer 11 the password for connection and identification code which were read by S5, and transmits. S6 carries out a password check. This compares the password for connection transmitted by S5 with the password for connection of the identification code concerned with which a password comparison means 14 of the connection place computer 11 by which identification code was received was read from the password storing field 16, and distinguishes the inside of a paddle in agreement. When in agreement, it progresses to S7. In the case of an inequality, a termination etc. carries out connection processing as an error.
[0027] Since S7 was proved that it is coincidence of S6 and became the check O.K. of a password, it makes computer connection. The connection place computer 11 connects this with a terminal 1. S8 creates a random number from the old password and a connect time. This creates a random number from the password for connection and connect time of old things [means / 5 / to constitute the password management equipment 2 of drawing 1 / password creation].
[0028] S9 creates the password for connection. This creates the password for connection based on the random number created by S8. S10 changes a connection password. This updates the old password for connection of the password storing field 8 while it transmits the password for connection which the password change means 6 of drawing 1 newly created to the connection place computer 11 and makes the old password for connection of the password storing field 16 update (modification) (modification).
[0029] When the password management equipment 2 which constitutes a terminal 1 connects with the connection place computer 11 by the above Using the password for connection, a user is checked (a principal with identification code and a password check), and it connects. Offer of service with a receptacle By newly creating the password for connection, and updating the password for connection in the password management equipment 2 by the side of a terminal 1, and the password for connection in the connection place computer 11 synchronously (modification) It is changed without a user being [the password for connection] automatically conscious for every connection. If it embezzles and connects while becoming possible to become a different password for connection next time, and to prevent thoroughly the surreptitious use over a long period of time, even if it acquires the password for

connection by the third party in secrecy, the password for connection will be changed. Even if it is going to connect using the password for connection from the user (password management equipment 2) of Shinsei, it becomes possible to become improper and to get to know having embezzled.
[0030] Drawing 4 shows the password change processing flow chart for connection of this invention. drawing 4 -- setting -- S21 -- modification initiation of a password -- it carries out. This starts modification processing of the password for connection of the password management equipment 2 of drawing 1 .
[0031] S22 enters an old password. S23 enters a new password. S24 stores a new password. Under the present circumstances, when in agreement with the present password with which the old password entered by S22 is stored in the password storing field 8 of drawing 1 , it is referred to as O.K., and a new password (password for connection) is stored in the password storing field 8, and the password for connection is changed (updating). In addition, when the password for connection stored in the password storing field 16 in the connection place computer 11 of drawing 1 is changed (updating) and the old password for connection is in agreement similarly, it changes with the new password for connection (updating).
[0032] When the old password for connection is in agreement with the above, it becomes possible for a third party to take care not to update the password for connection by changing the password for connection of the password storing fields 8 and 16 with the new password for connection created for every connection (updating).
[0033] Drawing 5 shows the creation explanatory view of the password for connection of this invention. In drawing 5 , the old password is a password for connection used now. Connection request time amount is an example value from which the password management equipment 2 of drawing 1 is the time amount which carried out the connection request, is YYMMDDHHMMSS (date time second ms), and always changes to the connection place computer 11.
[0034] The count of connection is a count which the password management equipment 2 of drawing 1 connected to the connection place computer 11, and is an example value which changes for every connection. Random-number-generation equipment 31 is well-known random-number-generation equipment which generates a random number based on the old password (old password for connection), connection request time amount, and the count of connection.
[0035] A new password is a new password for connection generated by random-number-generation equipment 31 from the old password, connection request time amount, and the random number generated based on the count of connection.
[0036] As mentioned above, it becomes possible to generate a random number the old password (old password for connection), the connection request time amount which always changes, and based on the count of connection which changes for every connection further, and to carry out automatic creation of the new password (new password for connection).
[0037]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is system configuration drawing of this invention.
[Drawing 2] It is an explanation flow chart of operation about this invention.
[Drawing 3] It is an example of a screen about this invention.
[Drawing 4] It is a password change processing flow chart for connection about this invention.
[Drawing 5] It is the creation explanatory view of the password for connection of this invention.
[Description of Notations]
1: Terminal (client)
2: Password management equipment
3: Password reading means
4: Connecting means
5: Password creation means
6: Password change means
7: Advice means of a connection result
8: Password storing field
11: Connection place computer
12: Connection processing activation means
13: Password reading means
14: Password comparison means
15: Advice means of a connection result
16: Password storing field
21: Terminal input unit
31: Random-number-generation equipment

[Translation done.]

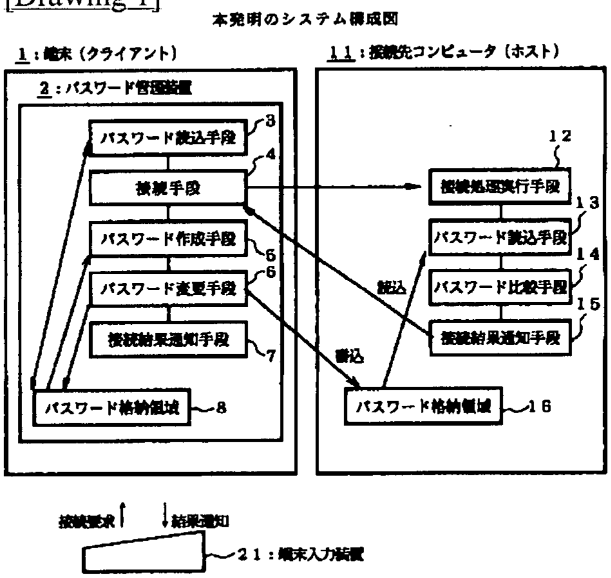
* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

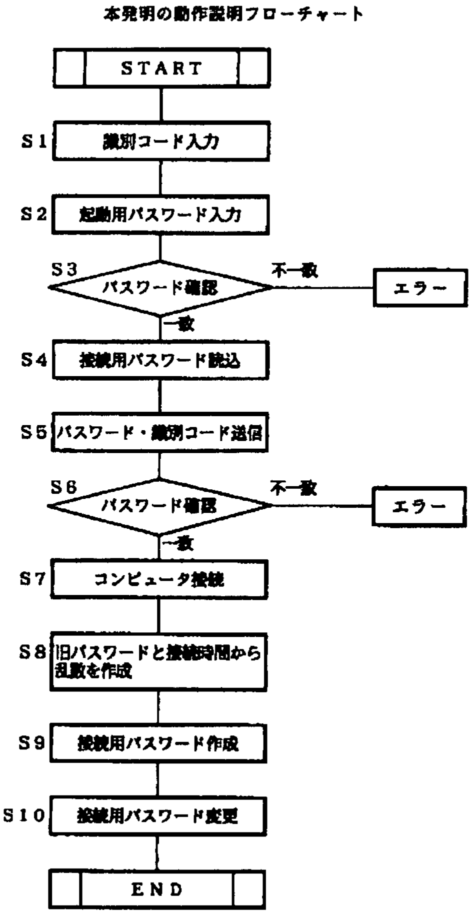
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

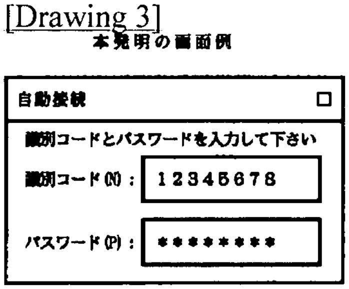
[Drawing 1]



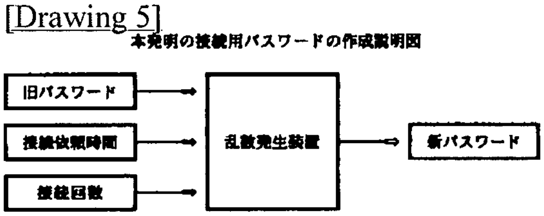
[Drawing 2]



[Drawing 3]

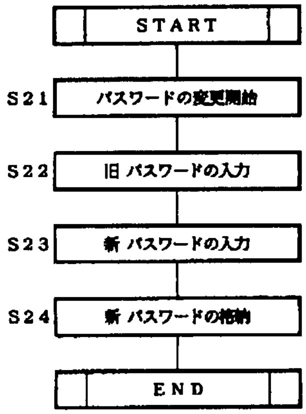


[Drawing 5]



[Drawing 4]

本発明の接続用パスワード変更処理フローチャート



[Translation done.]